



**ITACS**

**Information Technology and Communications Services**

Naval Postgraduate School, Monterey, California

## **New User's Guide to Information Technology and Communications Services**

*Updated 02 January 2004*

## Table of Contents

<a href="#">Services Provided</a> .....	3
<a href="#">Technology Assistance Center</a> .....	3
<a href="#">Public Labs/Classrooms</a> .....	3
<a href="#">Login Instructions</a> .....	4
<a href="#">User Responsibilities</a> .....	4
<a href="#">Computer Security Overview</a> .....	5
<a href="#">NPS PC Lab User Agreement</a> .....	6
<a href="#">Academic and Client Services Labs</a> .....	8
<a href="#">E-Mail with Microsoft Exchange &amp; Outlook – Overview</a> .....	9
<a href="#">Using Outlook for the First Time</a> .....	9
<a href="#">Forwarding Exchange Mail to Another Internet Address</a> .....	9
<a href="#">Logging into the NPS Exchange Mail via the Internet</a> .....	10
<a href="#">NPS Dial-Up Remote Access Services (RAS)-Windows</a> .....	11
<a href="#">NPS Dial-Up Remote Access Services (RAS)-Macintosh</a> .....	12
<a href="#">Additional Important Information Available on the Web</a> .....	13
<a href="#">NPS Policy on Appropriate Use and Standards of Conduct</a> .....	14

**Please send any comments/questions/suggestions/updates, etc  
Concerning this document to the Manager, Technology Assistance Center  
(TACMgr@nps.navy.mil)**

Last review: January 02, 2004  
Reviewed By: Chris Abila

## **Services Provided**

Windows and UNIX computers are available for use by students, faculty, and staff of NPS. This privilege does not extend to “guests” of authorized users, such as, spouses, children, friends, etc. Your computer account(s) is (are) exclusively for your own use.

Your computer account gives you a home directory for server storage of your files, access to software programs you will need, network access to the Internet and to the local NPS Intranet, and E-mail privileges using Microsoft Outlook.

Online E-mail assistance and information is provided at the following URL:

<http://www.nps.navy.mil/ITACS/email.htm>.

## **Technology Assistance Center (TAC)**

The Technology Assistance Center (TAC) is available to provide you with IT solutions. The TAC is located in Ingersoll Hall, Room 151, and is normally staffed Monday through Friday, 0800-1630.

You may report any IT problems you may encounter, by calling 656-1046, or by visiting the TAC in Ingersoll Hall, Room 151. You may also submit an IT Remedy case via the web at the following URL:

<http://www.nps.navy.mil/ITACS/Remedy.htm>.

## **Public Labs/Classrooms**

Your home directory is available from any Windows PC Lab on campus. PC Labs are open during normal business hours, Monday through Friday, 0800-1630.

After hours, Lab access is available via cipher lock. Cipher lock combinations are different for each Lab. Cipher lock combinations are issued by the Technology Assistance Center, Ingersoll Hall, Room 151 during normal business hours. See page 5 of this Guide for a list of public access Labs. Lab access combinations must not be shared with any other person.

Authorized users of NPS Labs have read the **NPS Appropriate Use Policy (NAVPGSCOLINST 5230.4C)**, and the **NPS NT Lab User Agreement**.

Both are included in this Guide. Refer any questions or problems you may have with IT services in the Labs you use, to the Technology Assistance Center (TAC).

## **Login Instructions**

Windows PC logon is initiated by simultaneously pressing the **Ctrl-Alt-Del** keys on any Windows computer. You will be prompted for your User name (sometimes referred to as your account name, or User ID), which is based on your first initial, middle initial, and the first six characters of your last name), and for your password. Passwords are case sensitive. Make sure you type your password in carefully, and correctly. To change your password, follow the instructions provided in this Guide.

## **User Responsibilities**

You are responsible for all activity on your account. Remember to log off the computer when you are finished working with it! You are required to abide by the **NPS Appropriate Use Policy (NAVPGSCOLINST 5230.4C)**, and the **PC Lab User Agreement**. Copies of these documents are included in this Guide. The Appropriate Use Policy can also be read at: <http://www.nps.navy.mil/ITACS/AppropriateUse.pdf>.

Computer use at NPS is intended **“For Official Use Only.”** That is, official, academic, and research use only. Incidental personal use is permitted for E-mail and Web browsing. NPS computers and/or networks may not be used for commercial or proprietary work. Specific restrictions limit your use of bulk E-mail (a message to 25 or more addressees). Refer to the Appropriate Use Policy for further guidance on this topic.

Software on NPS computers is copyrighted and may **NOT** be copied or redistributed for use on any other computer, unless specifically stated otherwise by ITACS personnel. Software may **NOT** be installed on NPS computers without the explicit consent of ITACS personnel.

Server disk space is a shared resource. You must manage your E-mailbox and home directory so that old files are archived or deleted, and server disk space is used efficiently. If an ITACS support person contacts you about archiving or deleting excess files on servers, please take immediate action.

You must unsubscribe from all mailing lists and/or discussion lists before you leave NPS. You must check out with the Student Services Center, located in the Basement of Herrmann Hall, during the week before you plan to leave NPS. This applies to **ALL** NPS employees. You can find the check out form at:

<http://www.nps.navy.mil/code03/Gradinfo/CheckoutSheet.doc>

A Pre-Departure Checklist is available, and is useful for all employees leaving NPS. You can find the Check-List at: <http://www.nps.navy.mil/ITACS/new/predepartcheck.htm>

You must uphold your User Responsibilities. Failure to do so will be reported, and your computing privileges may be revoked.

## **Computer Security – Overview**

NPS computer users are the front line of defense for custody, control, and confidentiality of all systems they use. The use of safe passwords, up-to-date anti-virus software, familiarization with appropriate use guidelines and lab rules, and the development and practice of sound user procedures, are all **essential** in protecting NPS IT systems from breach by non-authorized users. Internet connection enhances education at NPS, but exposes the user and NPS to greater security risks. Password cracking is the primary method used to penetrate systems connected to the Internet. Weak passwords, unsound practices, and carelessness, all cause security failures that defeat ADP Security protection programs.

Passwords suitable for stand alone office or home computers are usually not suitable for machines connected to the Internet. Passwords sent through the Internet SHOULD BE CHANGED VERY FREQUENTLY. Non-encryption processes are used on some IT systems at NPS, for remote login access and Internet traffic. From source to destination, passwords are subject to multiple intercepts and observations. Passwords used for dial-in connection to NPS are considered reasonably secure, and thus need to be changed only periodically. If the same password is used for remote Internet access though, (normally the case) the password should be changed more frequently.

Complete guidance on password policies and procedures at NPS may be found at: <http://intranet.nps.navy.mil/Code05/New05/pwldr.htm> (internal only).

**Note: Some of the web pages referenced in this document are only available via the NPS Intranet. They cannot be accessed from off campus sites, unless you are connected via dial up LAN access.**

## **NPS PC LAB USER AGREEMENT**

ITACS, Academic and Client Services (ACS) maintains Windows based Labs, in order to provide computing services to faculty, students and staff. You must have an NPGS domain account to use the PC computing facilities. Users will not give out passwords to their NPGS accounts. If you suspect that your password has been compromised, contact the Technology Assistance Center (TAC), Ingersoll Hall, Room 151 for assistance in changing your password.

**Windows PC computing laboratories which have been standardized on the NPGS domain are located in SP-105, SP-243, SP-263, SP-431, HA-201D, RO-204, RO-204a, RO-228, ING-151, and GL-128.**

Other laboratories exist throughout the campus, using a variety of computing platforms. Some of these "other" labs are designated exclusively for the use of students from particular classes. Professors will let students know if they have access to labs not mentioned in this agreement.

The use of the ACS Labs is restricted to those who have read and agreed to this **NPS PC Lab User Agreement**. The ACS Labs are not available for use by "guests" of authorized users, such as spouses, children, friends, fellow students, etc.

The ACS Labs are open during the normal work day, Monday through Friday, 0800 - 1630. After hours access is available via cipher lock combination. Combinations are issued to authorized users by the Technology Assistance Center (TAC). Users should not distribute combinations. Do not allow Lab access to anyone who requests entry, and does not already have the combination.

A sign-in log is used for after hours access. When you use the Lab after normal working hours, you must sign in and out of the Lab on the access log. **The doors to the ACS Labs must remain closed and locked after normal working hours have ended.**

All software installed on ACS computers is copyrighted and **may not be copied** or redistributed for use on other on-campus or off-campus computers. Access to the ACS Labs may be denied to anyone guilty of copyright violation. **No applications, including freeware, shareware, plugins, etc., shall be installed on ACS computers without the expressed consent of the ACS staff.**

All users are required to abide by the NPS Appropriate Use Policy (NAVPGSCOLINST 5230.4C), which can be found at <http://www.nps.navy.mil/ITACS/AppropriateUse.pdf>. Copies of this instruction are also posted in all ACS labs, and are included at the end of the New User's Guide.

All computers at the Naval Postgraduate School are Department of Defense (DoD) computer systems. These computer systems, including all related equipment, network, and network devices (specifically including Internet access), are provided only for authorized U.S. Government use. The use of DoD computer systems at NPS, authorized or unauthorized, constitutes consent to the monitoring of these systems. Violations of any part of this agreement will be reported to the appropriate authority.

## **Academic and Client Services Labs**

### **NPGS Domain**

Spanagel Hall PC Labs (Sp-105 & Sp-431)

Spanagel Hall PC Labs (Sp-243 & Sp-263)

Halligan Hall PC Lab (Ha-201D)

Root Hall PC Labs (Ro-204, Ro-204A, R0-228)

Ingersoll Hall PC Lab (In-141)

Glasgow Hall PC Lab (Gl-128)

### **PC Labs – Not Standard Configured for NPGS Domain**

Ingersoll Hall Windows 95 Lab (In-224) and Ingersoll Hall NT PC Lab (In-250)

### **Labs Using Other Platforms**

Root Hall IDEA Lab with SGI computers (Ro-234S)

Mechanical Engineering Bldg, Mixed Platform Lab (Me-138)

Glasgow Hall PC/UNIX/HP Lab (Gl-318)

For assistance, contact the Technology Assistance Center (TAC), at 656-1046.

## **E-Mail with Microsoft Exchange & Outlook – Overview**

Exchange is the name of the Microsoft mail **server** software in use at NPS. Outlook is the Microsoft mail **client** software (GUI). Outlook is an integrated product supporting Email, calendars, contacts, and task management. Outlook Express is not the same product, and should not be used for your primary E-mail activities. NPGS account holders will use Outlook to read their E-mail at NPS.

Your E-mail address consists of your User name (first initial, middle initial and the first 6 letters of your last name) and the NPS Hostname (nps.navy.mil). For example: E-Mail for John G. Newuser would be addressed to [jgnewuse@nps.navy.mil](mailto:jgnewuse@nps.navy.mil).

Your personal archive file (archive.pst) and your personal address book file (mailbox.pab) are stored in your home directory, in the path H:\exchange. Do not move these files. These files are backed up daily on NPS servers.

You can access your Exchange E-Mail from **any Internet-connected computer, anywhere in the world**. Direct your Internet browser to:  
<https://itwarrior.nps.navy.mil/exchange>.

### **Using Outlook for the First Time**

Ensure your archive file and your personal address book files are located in the correct path. You can check this by double clicking the “My Computer” icon on your desktop, and then double clicking the (H:) icon. Your archive.pst file and mailbox.pab file should both be in the “Exchange” folder. Close the window.

Double click the Microsoft Outlook icon on your desktop to open Outlook. If you have any difficulty, call the Technology Assistance Center (TAC), at 656-1046.

### **Forwarding Exchange Mail to Another Internet Address**

As of 22 October 2001, in order to provide a secure and contained environment for Official Use Only e-mail, and to prevent uncontrolled distribution of potentially sensitive information via e-mail, [automatic forwarding of mail](#) to an off campus email account is no longer permitted.

## **Logging Into NPS Exchange Mail Via the Internet**

Open your web browser (Netscape or Internet Explorer).

Type in this URL in the address field: <https://itwarrior.nps.navy.mil/exchange>

The NPS Outlook Web Access (OWA) logon page opens up.

You will be prompted for your User name. Enter your email address (minus '@nps.navy.mil').

The "Enter Network Password" screen will appear.

Type your User name (Network login) in the blank field.

TAB, then type in your account password, and press "Enter".

You are now logged into the Exchange server remotely, via a 128-bit secure encryption Internet connection. You can read your email, calendar, browse the public folders, your contacts file, etc. However, you will not be able to use your Personal Address Book or Personal Distribution Lists.

It is very important to **log off of the Exchange server** when you are done. Just click on the Log Off icon at the bottom of the left hand frame. This closes the secure connection.

## **NPS Dial-Up Remote Access Services (RAS) Windows**

These instructions allow the **authorized** Naval Postgraduate School user to establish a connection to the NPS Information Technology Remote Access Server in order to access e-mail through a standard telephone.

### **NPS Local Area Telephone Connection:**

When connecting to the NPS Remote Access Server (RAS) from a Windows computer, a dial-up connection must be configured. To do this, the following steps must be accomplished:

#### **Configure the Microsoft Client**

1. Select My computer and Control Panel. Select the Network Icon and double click on the Microsoft Client. (If the Microsoft Client is not installed, select Add|Client|Add|Microsoft and OK and Close out of the Wizard.

2. Check the block to logon to the Domain and enter in Caps (NPGS) for the name of the domain.

#### **Configure/Add the Dial-up Adapter.**

1. Select My Computer and Control Panel. Select the Network Icon. Double click the Network Icon.
2. To Add the Dial-up Adapter. Select Add|Adapter|Add Dial-up Adapter, OK.
3. At this point you may be asked to put the Windows CD in the CD-ROM drive.

#### **To add a New Dial-Up Connection**

1. Double click the "My Computer" icon on the desktop.
2. In the "My Computer" window, double click "Dial-Up Networking."
3. The "Dial-Up Networking" window will appear. Double click "Make New Connection.
- 12
4. The "Make New Connection" dialogue box appears and you are prompted to name the connection. The name "NPS-RAS" is recommended. Then click "Next".
5. You are then prompted to enter the telephone number for the computer to call. Enter **656-4695** and click "Next." (This is the number for the hunt group.)
6. You will then see the final screen which indicates that you have successfully created a new Dial-up Networking connection. Click "Finish."
7. You may then elect to create a shortcut to this connection on the desktop. To do so, locate the icon for the connection you have just configured in the "Dial-Up Networking" window and right click on it. Select "Create Shortcut" from the drop-down menu. You will be notified that you cannot create a shortcut here. Click "Yes" to place the shortcut on the desktop.
8. Double clicking this icon will initiate your connection to the NPS-RAS server. You will be prompted to enter your username and password to log into the NPGS domain of the School's Windows NT network. For security reasons, DO NOT select "Save password." Doing so will allow anyone access to your e-mail and Windows NT account at anytime.

**Long Distance/TAD Telephone Connection:**

When connecting to the NPS-RAS server while on travel **away from the NPS local area**, a dial-up connection via **1-800** telephone service is available. To do this, follow the instructions above, substituting **800-656-2944** for the phone number in step 5.

**To map to your Home directory:**

Right click on the My Computer Icon and select Map a network drive. Select the drive letter H for Home directory. In the path field enter \\server name\username\$. Check the Reconnect at logon box to reestablish the connection each time you logon.

## **NPS Dial-Up E-Mail Remote Access Services (RAS) Macintosh**

Using ARA (Apple Remote Access) in current version of MAC OS 8.6 and above.

Control Panel, remote access. Enter NPGS domain Login and Password.  
Option to save password.

Phone numbers are the same as Windows, above.

Connect via RAS using DHCP. In Control Panel, set TCP/IP to PPP.

Gives Mac access via TCP/IP to NPS, allowing the use of Internet browser, connection to Outlook/Exchange Mail system, POP mail (mail.nps.navy.mil).

## **Additional Important Information Available On the Web**

Technology Assistance Center

<http://www.nps.navy.mil/ITACS/TAC.htm>

Information Security

(Required All Hands Reading)

<http://intranet.nps.navy.mil/Code53/InfoSec/alerts.htm>

The NPS Intranet

<http://intranet.nps.navy.mil>

Information Technology and Communications Services

<http://www.nps.navy.mil/ITACS/>

Microsoft Exchange Mail Services

<http://www.nps.navy.mil/ITACS/email.htm>

## NAVPGSCOL INSTRUCTION 5230.4C

Subj: POLICY ON APPROPRIATE USE OF NAVAL POSTGRADUATE SCHOOL  
COMPUTING AND INFORMATION SYSTEMS

Ref: (a) Department of Defense (DoD) Web Site Administration  
Policies and Procedures  
(b) OPNAVINST 5300.8B  
(c) Department of Defense (DoD) Instruction 1100.13,  
Surveys of DoD Personnel  
(d) SECNAVINST 5720.47

1. Purpose. To establish general Naval Postgraduate School (NPS) policy on appropriate use of NPS computing and information systems, and standards of conduct for users of those systems, consistent with the NPS mission and Department of the Navy/Department of Defense (DON/DoD) guidelines.

2. Cancellation. NAVPGSCOLINST 5230.4B

3. Applicability. This instruction applies to all users of computer and information systems owned or operated by NPS, its tenant commands and activities. It also applies to users of any computer or information system, regardless of ownership, that is either remotely or directly connected to the NPS network.

### 4. Background

a. The principal mission of NPS is graduate education. To properly execute this mission, NPS must support the intellectual and professional growth of its faculty, staff and students. NPS is also a military command within DON/DoD and must, therefore, operate under Federal and DoD guidelines. These guidelines specify that Government resources, including computer and information systems, may be used for authorized, "official" purposes, only.

b. The expanded use of the Internet, electronic mail, and web technology provide the individual user an almost unlimited capability for communication and rapid access to, and transfer of information. In taking full advantage of the opportunities

that these technologies provide, the boundaries between appropriate (official) and inappropriate uses can frequently become blurred. The need to clarify these boundaries requires that NPS define clear and explicit policies on appropriate and acceptable use of its computer and information systems.

## 5. Policy

a. In consideration of its primary educational mission, NPS authorizes use of its computing and information system resources for all purposes reasonably related to graduate education and research; to intellectual and scholarly inquiry; to the NPS military mission; and to the general professional interests and growth of its faculty, staff, and students. Faculty, staff, and students are encouraged to make maximum use of these resources for expanding their professional horizons, and for increasing their knowledge, skills, and ability to contribute to NPS and to the community at large. Minimal incidental and innocuous use of these resources for personal study and communications that contribute to generally increasing those computer and information resources skills crucial to education, research, and professional development is also authorized.

b. NPS restricts only those uses of its computing and information system resources that are clearly inappropriate in a taxpayer-supported institution, or which are clearly inconsistent with the professional standards expected of its faculty, staff, and students. In any instance involving a question as to whether a specific action or conduct is or was appropriate, the primary consideration should be whether such action or conduct would be consistent with that expected of military officers, scholars, public servants, and members of the professional academic community, who realize that their actions reflect not only on themselves, but on NPS and DoD as well.

c. Network monitoring tools are used to obtain detailed information relating to network performance, security vulnerabilities, and the amount and types of usage. This information can be used to monitor compliance with School policies, including appropriate use. All users should be aware that NPS computer and information systems and networks are subject to monitoring at all times, and that use of these resources implies consent to such monitoring. Consequently, no

expectation of privacy should be assumed regarding information transmitted, received, or placed in NPS systems. Violations of the policies defined herein may subject the user to disciplinary action.

## 6. Specific Restrictions and Limitations

a. General. While individual computer system administrators normally define the parameters for use of their respective systems, there are certain activities so clearly not in keeping with the NPS mission or its status as a professional graduate school that they are expressly prohibited on all systems to which this policy applies. These are:

(1) Illegal, fraudulent, or malicious activities; partisan political activity; political or religious lobbying or proselytizing; or activities on behalf of organizations having no acknowledged affiliation with NPS; or, activities which result, or might reasonably be expected to result, in an allegation of harassment of an individual or group, regardless of their affiliation with NPS.

(2) Activities for the purpose of personal or commercial financial gain. This includes solicitation of business, services, or commercial products; conduct whose purpose is to further or support these activities.

(3) The use of any NPS computing resource for the purpose of transmitting or displaying inappropriate, offensive, or obscene language or material such as pornography, racial or ethnic slurs, personal insults, "hate literature", etc.; accessing, downloading, or storing files or material of a similar nature.

(4) Storing or processing classified information on any system not explicitly approved for classified processing.

(5) Using another individual's account or identity without their explicit permission.

(6) Viewing, modifying, or deleting other users' files or communications without appropriate authorization or permission.

(7) Activity for the purpose of circumventing or defeating the security or auditing functions of any system; surreptitious probing or examining of any system for the purpose of penetrating or disclosing security vulnerabilities of that system; or, the use of any program or utility for the purpose of conducting such activity, except as may be specifically authorized by the Superintendent, and only as part of legitimate system testing, security research, or in the performance of assigned security-related duties.

(8) Obtaining, installing, storing, or using software obtained in violation of the appropriate software license or copyright, or allowing unauthorized individuals to access or use NPS-licensed software in violation of the licensing agreement (i.e., software "piracy").

(9) Modifying or altering the operating system or configuration of any NPS system, including the installation of software, without first obtaining permission from the custodian or administrator of that system.

(10) Disclosing User IDs and Passwords, or otherwise permitting or enabling any unauthorized individual to access an NPS system.

(11) Storing, processing or displaying Sensitive Unclassified information, such as Privacy Act information or For Official Use Only, on systems which do not provide the appropriate protection for such material, or failing to adequately and prudently protect such material when it is stored, processed or displayed on appropriate systems.

b. There are certain other activities, which while not absolutely prohibited, are almost always inappropriate. Individuals engaging in them may be asked to justify their activities, and if reasonable justification does not exist may find their judgement and/or professional standards seriously questioned. Examples of such generally inappropriate activities are:

(1) Use of NPS systems that, in the judgement of the responsible system administrator, seriously interfere with other, legitimate uses or users. Examples include "hogging" systems for non-academic purposes (e.g., game playing); excessive large file transfers; excessive personal e-mail;

excessive storage of large (e.g., multi-media) files;  
storage of non-academic files, etc.

(2) Inconsiderate conduct toward other system users.

(3) Storing files or material that could be used for illegal or fraudulent purposes.

b. Web Pages. In addition to the general prohibitions cited above, the following policies specific to Web pages are also established:

(1) NPS Web servers may only be used for official business, and in an official capacity.

(2) Personal Web sites hosted by commercial Internet Service Providers (ISPs) will not be used for official purposes.

c. E-Mail. E-Mail originating from NPS systems establishes the sender's affiliation with NPS and the DoN/DoD. For this reason, such communications may be construed as being official in nature, or expressing official NPS or DoN/DoD policies or views. Users should also be aware of the capacity for their communications to reach a mass, even global, audience, or to be forwarded to unintended recipients. Users are expected to exercise appropriate discretion in the use of e-mail on NPS systems, in accordance with the following guidelines:

(1) E-mail will not be used to circumvent or bypass the normal chain of command for official actions.

(2) Originating, broadcasting or forwarding of chain letters or unsubstantiated security or virus alerts is prohibited.

(3) E-mail attachments should be scanned for viruses before transmission.

(4) The use of mass-mailing (defined as having 25 or more addressees) to multiple curriculums or departments on campus is authorized provided the subject matter reasonably relates to the legitimate academic or professional interests of the target audience, and is approved by the responsible

curricular officer or department head; mass-mailings off campus must be approved by the Superintendent or his designated authority.

(5) E-mail to bulletin boards, discussion groups or other subscription lists is exempt from specific approval provided users generally limit such participation to forums related to their own academic or professional expertise, and ensure their contributions are restrained, professional, objective, and clearly identified as personal opinions, rather than those representing official NPS or DoN/DoD views.

(6) The use of e-mail to initiate or conduct surveys may be authorized provided the surveys are conducted in accordance with reference (b) or (c), as applicable, and adhere to the guidelines set forth in this instruction; all surveys originating at NPS are subject to review by the NPS Staff Judge Advocate.

## 7. Responsibilities

a. Department heads, managers, and supervisors have the primary responsibility for implementation of these policies, and for ensuring that:

(1) This instruction receives appropriate dissemination, and that personnel under their authority are familiar with these policies, and that these policies are enforced within their respective departments and work centers.

(2) Appropriate mechanisms for reporting violations are implemented, and that the Command Information Systems Security Manager (ISSM), Code 005, is advised of any alleged violations.

b. Users of NPS computer and information systems are responsible for compliance with these policies, and reporting suspected or alleged violations via their chain of command.

8. Action. Maximum use will be made of available mechanisms for electronic distribution of this instruction within each department. Time lines for actions to be completed are as follows:

a. Within 45 days of the date of this instruction Line Managers and Department Heads will:

(1) Ensure that all NPS faculty, staff, and/or students under their authority read this instruction, and sign an acknowledgement that they understand and will comply with the policies set forth.

(2) Develop and implement procedures to ensure all new faculty, staff, and students, etc., are briefed on these policies, and sign an acknowledgement, before being granted access to any NPS or network resource to which this instruction applies.

(3) Ensure that student and faculty handbooks, user manuals, and standard operating procedures, etc., are updated, as appropriate, to reflect these policies.

b. Within 60 days of the date of this instruction, and annually thereafter, the NPS Information Systems Security Manager will verify that all departments have completed the actions specified, and submit a report of findings to the Superintendent.

/s/  
ROGER L. BUSCHMANN  
By direction

Distribution:  
NAVPGSCOLINST 5605.2S (List 1)